



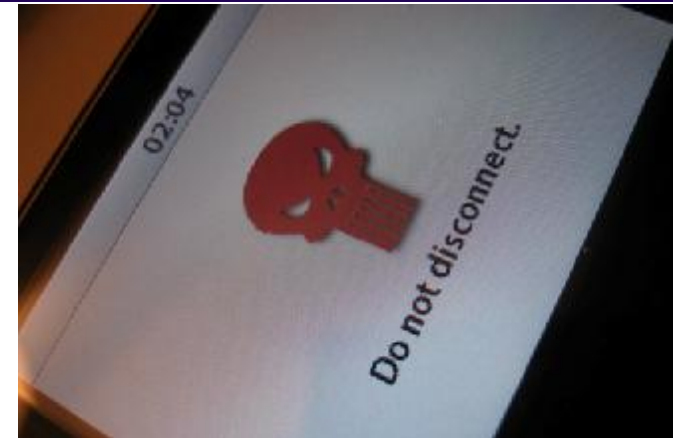
Insider Threats – A Taxonomy

**Making Sense of
Risk**

20th May 2010



- Insider Threat – What is it?
- What is the problem?
- What are the motivators?
- How do we fight it?



The screenshot shows a Twitter interface. At the top, the Twitter logo is on the left, and navigation links (Home, Profile, Find People, Settings, Help, Sign out) are on the right. A tweet from user 'theconnor' is shown, with a profile picture of a man in a suit. The tweet text reads: 'Cisco just offered me a job! Now I have to weigh the utility of a fatty paycheck against the daily commute to San Jose and hating the work.' Below the tweet are the options 'about 19 hours ago from web · Reply · View Tweet'. A reply from user 'timmylevad' is shown below. The reply text reads: 'I'm sure they would love to know that you will hate the work. We here at Cisco are versed in the web.' Below the reply is the user's profile picture and name 'timmylevad' with the real name 'Tim Levad' underneath. The background of the screenshot is a collage of various logos including 'eBook', 'You Broadca', '360°', 'EBO', 'flickr', 'pace.com', 'place for friends', 'ed in', and 'ebd'.

Case:

- Top foreign currency trader working for an investment firm
- Theft of \$691 million over five years, kept hidden



Analysis:

- Seen as “Star Performer” – above suspicion. Irrate when questioned.
- Both trader and programmer of software used to commit crime



Head of Fraud, Risk & Compliance @ MWR InfoSecurity
20 years in Information Security

Interests:

- Enterprise Risk Management
- PCI DSS
- Security Architecture
- Fraud Investigations

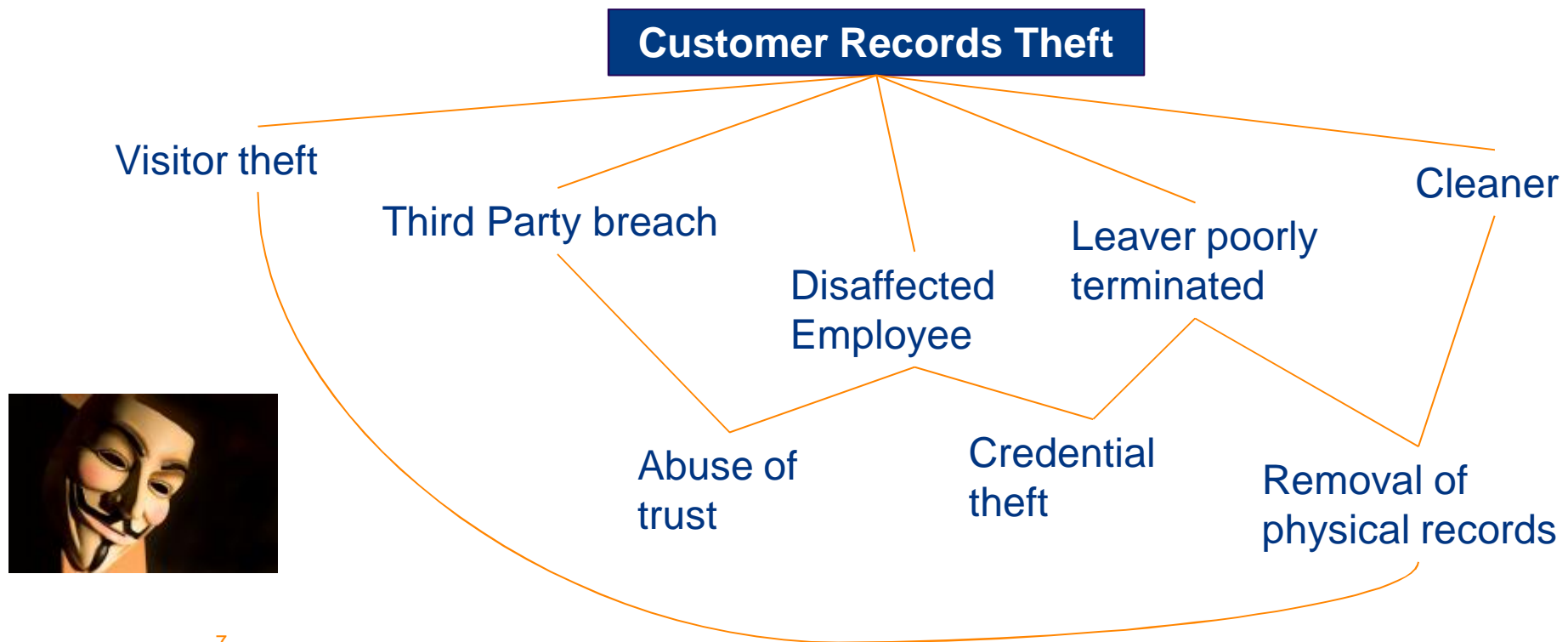
Former CESG Listed Advisor
Certified Fraud Examiner (CFE) and
BS7799 Lead Auditor, ITIL Security Practitioner



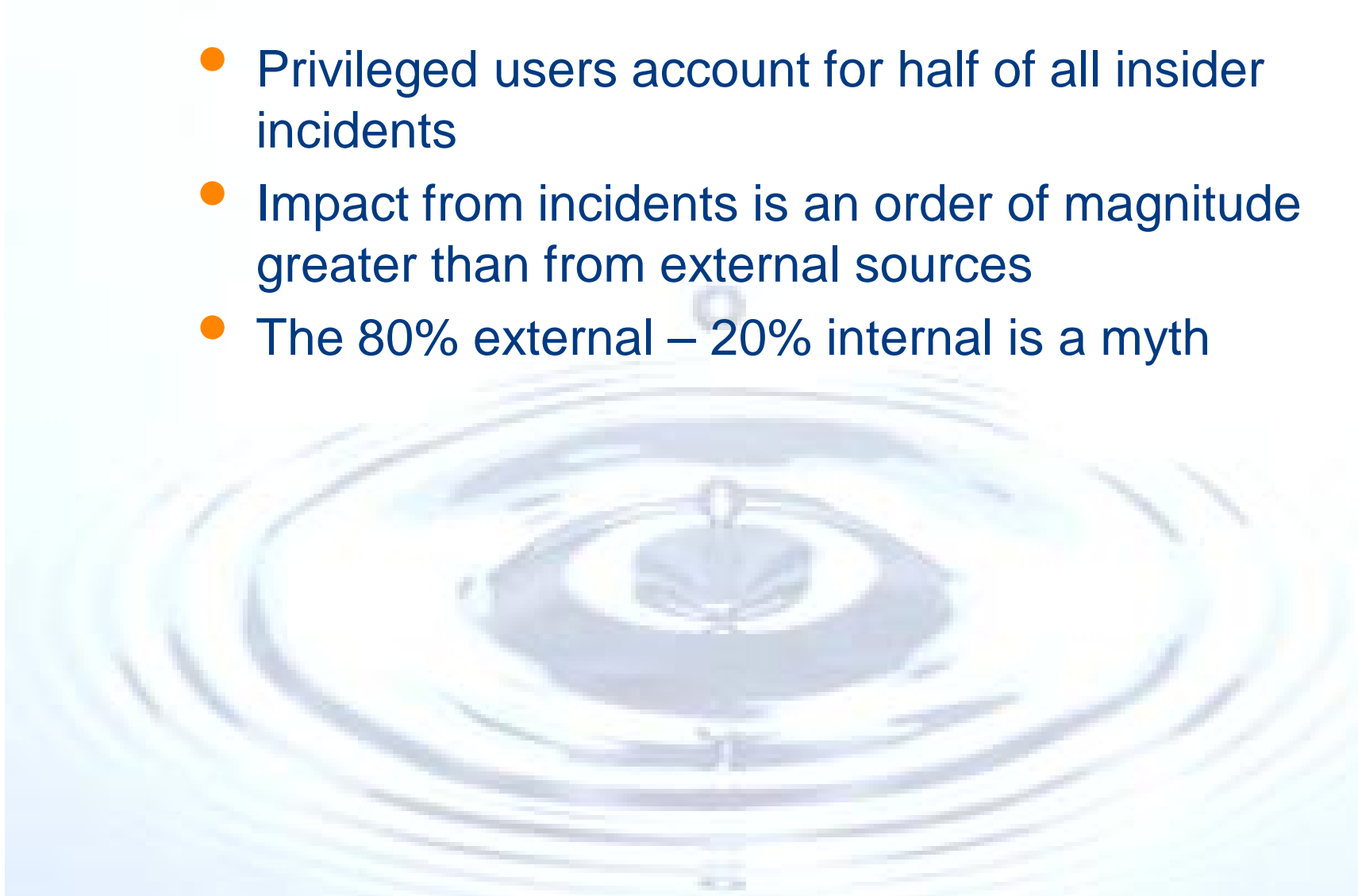


WHAT IS THE PROBLEM?

- An attack that (ab)uses a position of trust
- Gains unauthorised access to business assets
- A type of *Advanced Persistent Threat*



- Privileged users account for half of all insider incidents
- Impact from incidents is an order of magnitude greater than from external sources
- The 80% external – 20% internal is a myth



Source: Verizon data breach report

- Blending of Work and Personal Life
- Inconsistent enforcement of Policies
- IT doesn't own and control all devices
- Blurring of Internal vs. External
- Covert Attacks
- Moving Targets!



- “We Trust our Employees”
- “We have an open environment. We cannot clamp down.”
- “Insiders? Malware is ripping us to shreds”
- “Its an IMPOSSIBLE task!”
- “We use principle of least privilege, separation of duty, and pray. Lots.”



- A has presence in Russian Energy market
- B wishes to gain presence in market
- B hires key employee from A, deploys as head of Russian Energy.
- Key employee is alleged to have brought extensive confidential information belonging to A.
- A sues B for loss of business, hires computer forensics to perform electronic discovery, engages expensive lawyers





WHAT ARE THE MOTIVATORS?

(And how do we not go nuts doing it?)



- How do we identify a rogue team member?
- What organisational failures can create a situation where harm can be done by a disgruntled insider?
- How to promote positive company values alongside a security awareness culture

Theft of Confidential Information

- Leavers
- Disgruntled employees

IT Sabotage

- Insider has predisposition to commit the crime
- Over 30% have an arrest history (background check?)
- Hold grudges, “Act Out”, perform poorly, late for work

Fraud

- Single point of control over payments
- No visibility of process
- Never takes holiday
- “Hero”



Attack	Reported stresses
DOS	Loss of mentor at work, feeling exploited, replaced
Destroy HR data	Romantic Rejection, betrayal, loss of job, embarrassment at being caught on video breaking rules and lying
Hack POS databases	Loss of job without warning, loss of pay for periods worked, loss of access to computer resources
Theft of Client trading database	Feeling betrayed, criticised, fired by co-workers he thought were friends
Time bomb in manufacturing	Demotion, co-worker conflict, family death, illness
Extortion via PPI	Professional and financial frustrations – being stuck remotely
Hack into Inventory DB, time bomb	Co-worker conflict, demotion, criminal activity
Steal Engineering data	Family split, lack of training, probation
Snoop email / vM	Financial stress, marital problems, conflict w/ mgmt
Password to safety systems	Family illness, loss of control, alcoholism, conflict w/ mgmt and co-workers

Attack	Detection Delayed	Subject OPSEC	Time employed	Advance knowledge	Intervention
DOS	N	Y	2 months	2 months	2 weeks
Destroy HR data	Y	Y	34 months	16 months	16 months
Hack POS databases	N	Y	4 months	1 month	None visible
Theft of Client trading database	N	N	18 months	7 months	12 days
Time bomb in manufacturing	N	Y	11 years	4 years	14 months
Extortion via PPI	N	Y	N/A	N/A	N/A
Hack into Inventory DB, time bomb	Y	Y	2 months	1 month	1 month
Steal Engineering data	Y	Y	19 months	6 months	6 months
Snoop email / vM	N	Y	22 months	2 months	2 months
Password to safety systems	N	Y	15 years	19 months	19 months

Attack	Screening	Prior offenses / undetected factors	Tracked by HR?
DOS	Referred by brother, no check	No	No
Destroy HR data	No check	Multiple prior: forgery, theft, fraud, disorderly conduct	Yes
Hack POS databases	No check	Prior conviction, published hacker	Yes
Theft of Client trading database	No check	No	No
Time bomb in manufacturing	No check	No	No
Extortion via PPI	N/A (overseas)	No	No
Hack into Inventory DB, time bomb	Delayed background check	Prior hacking, extortion	Yes
Steal Engineering data	No check, recommendation	Published hacker	No
Snoop email / vM	No check	Yes (juvenile)	No
Password to safety systems	Hired by father, no check	No	No

Attack	Stress?	Conflict?	SPOF?	Policy lack	Enforcement
DOS	Y	Y	Y	Y	N
Destroy HR data	Y	Y	Y	Y	Y
Hack POS databases	Y	N	Y	Y	N
Theft of Client trading database	Y	N	Y	N	Y
Time bomb in manufacturing	Y	N	Y	Y	Y
Extortion via PPI	Y	N	N	N	Y
Hack into Inventory DB, time bomb	Y	Y	Y	Y	Y
Steal Engineering data	Y	Y	N	Y	Y
Snoop email / vM	Y	Y	Y	Y	Y
Password to safety systems	Y	Y	Y	Y	Y



HOW DO WE FIGHT IT?



How to motivate staff and detect aberrant patterns

- Tolerate, Prevent, Block, or Investigate

How to identify assets at risk?

Key risk reduction controls:

- Unique ID's across the enterprise
- Timestamping
- Unified log management
- Intrusion Detection
- Role-based Access Control (RBAC)

Clear identification of *Who* accessed an asset *When*
Policy statement requires careful thinking:

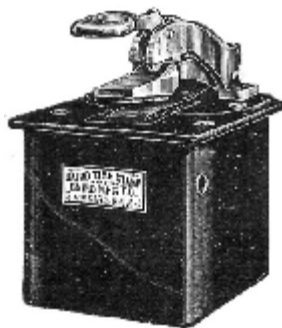
- Remote login as root or Windows Administrator?
- How to tie up authentication with:
 - Radius (VPN / RAS)
 - Desktop / File / Print
 - Applications
 - Databases (?)
- What do we do with our remote maintenance vendors?



Allows us to see who did what , *at what time*.

Heterogeneous systems are still a problem!

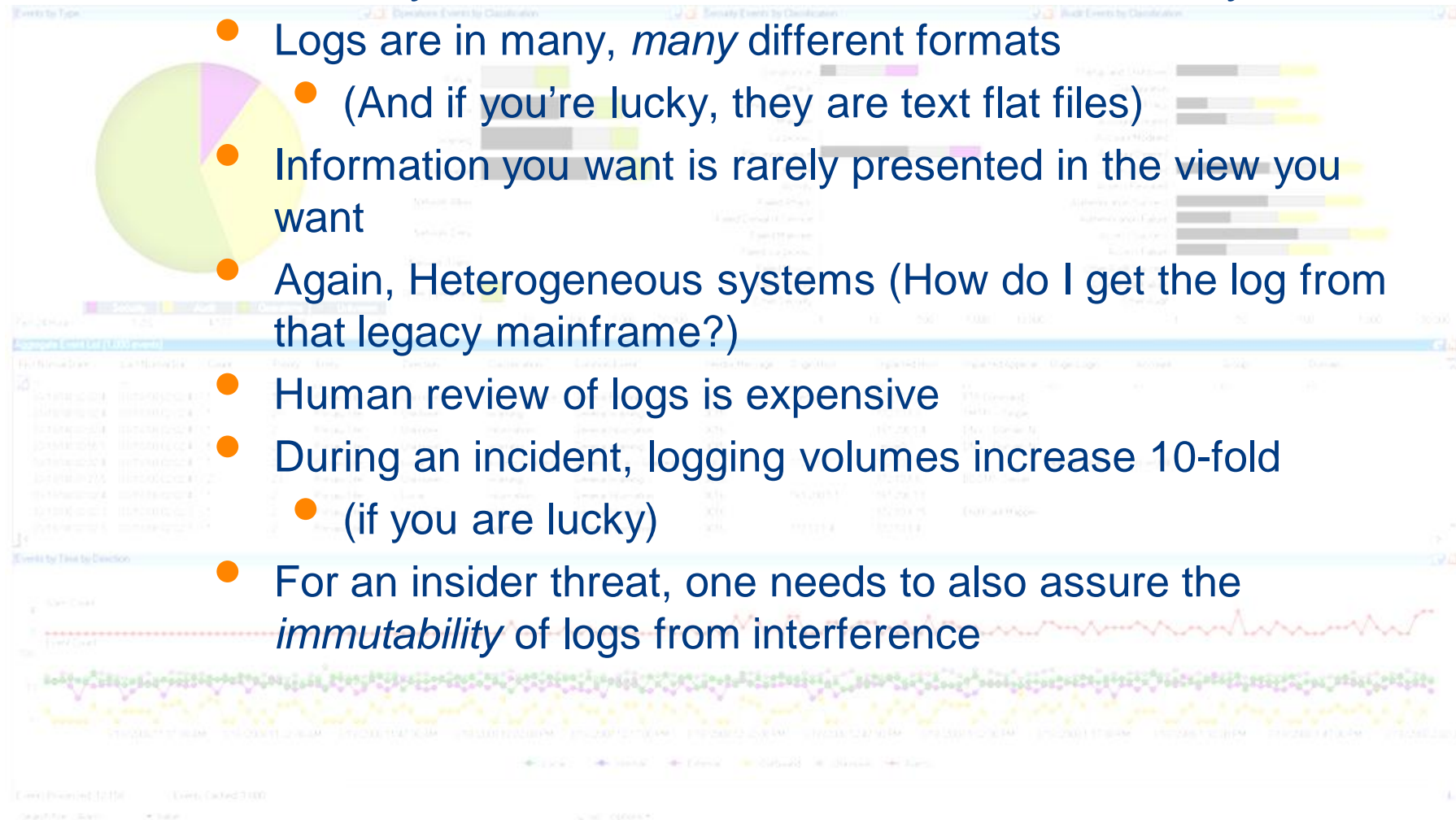
- Most data layer and application layer systems will pick up time from the platform
- NTP and AD do interoperate
- Do you run NTP autokeying?
- Pulling the information out of Windows can be...



```
' This code prints the last logon timestamp for a user.
' ----- SCRIPT CONFIGURATION -----
strUserDN = "<UserDN>" ' e.g. cn=rallen,ou=Sales,dc=rallencorp,dc=com
' ----- END CONFIGURATION -----
set objUser = GetObject("LDAP://" & strUserDN)
set objLogon = objUser.Get("lastLogonTimestamp")
intLogonTime = objLogon.HighPart * (2^32) + objLogon.LowPart
intLogonTime = intLogonTime / (60 * 1000000) intLogonTime =
intLogonTime / 1440 WScript.Echo "Approx last logon timestamp: " &
intLogonTime + #1/1/1601#
```

The “dirty little secret” of Information Security!

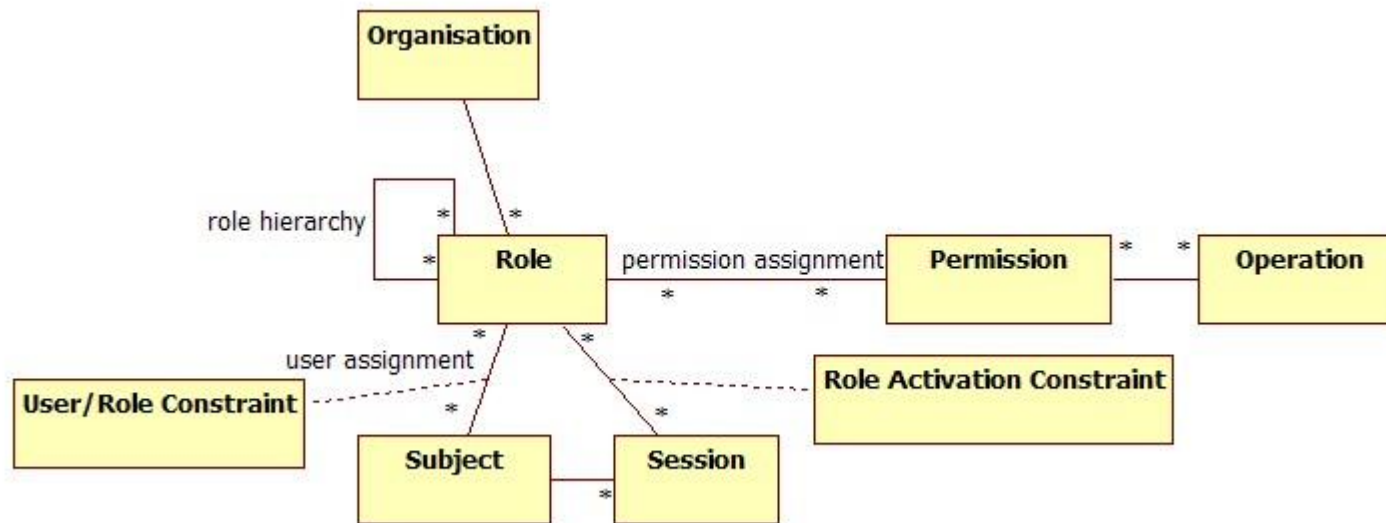
- Logs are in many, *many* different formats
- (And if you're lucky, they are text flat files)
- Information you want is rarely presented in the view you want
- Again, Heterogeneous systems (How do I get the log from that legacy mainframe?)
- Human review of logs is expensive
- During an incident, logging volumes increase 10-fold
 - (if you are lucky)
- For an insider threat, one needs to also assure the *immutability* of logs from interference





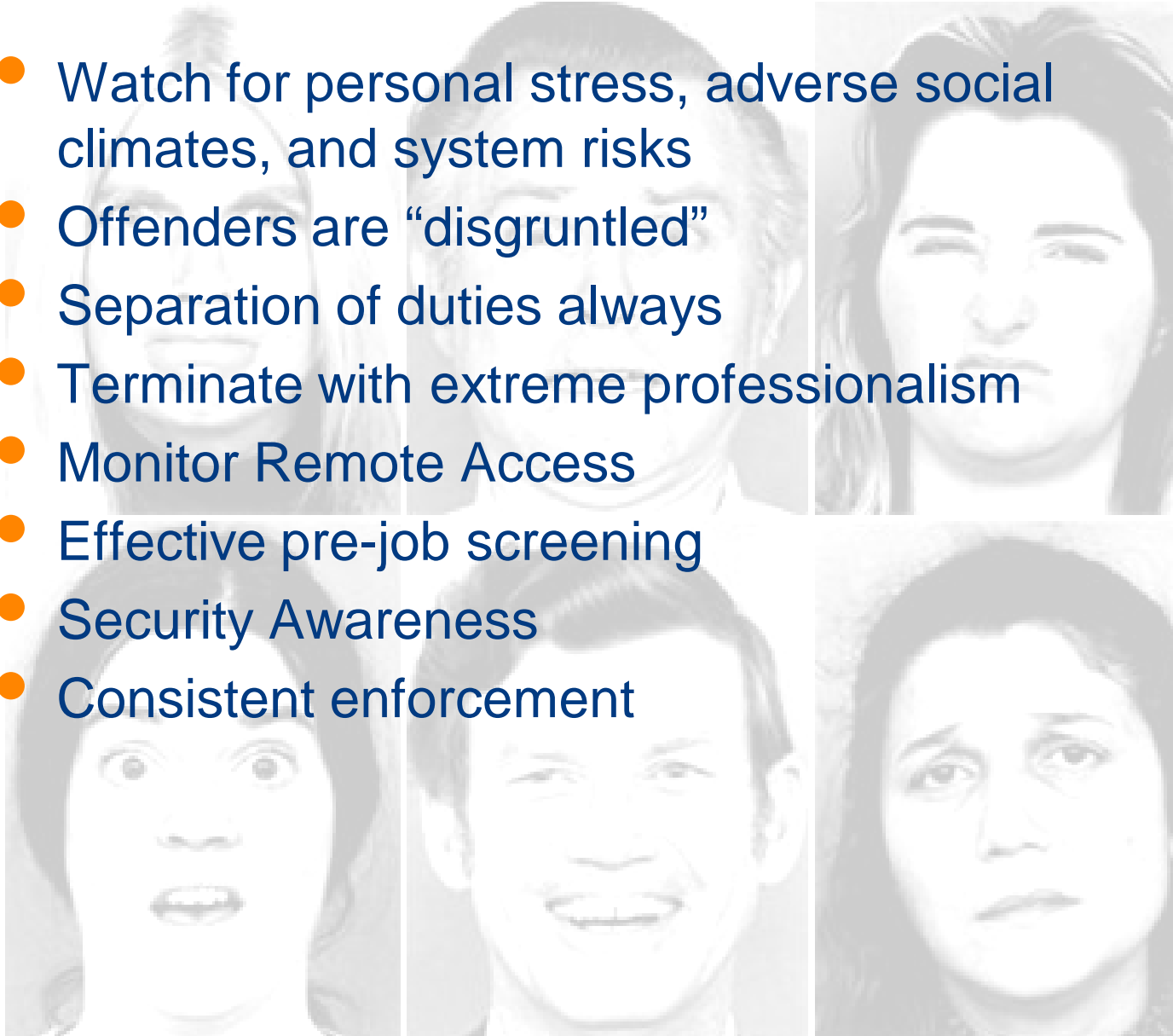
- “Detection .. Is undecidable and NP-Hard” - *Fred Cohen*
- IDS systems attempt to rate activity from normal to misuse
 - Modelling uses imperfect and incomplete information (how many events?)
 - Non-modelling approach uses heuristics, clustering algorithms, and statistics
- Types of attack
 - **External** - Intruders, Masquerader
 - **Internal** – Malfeator, Clandestine user

- Requires implementation of the technical controls above
- If we get it right, means people have the data required to do their job
- Combination of enterprise application controls, data layer controls, and network / platform controls





- Watch for personal stress, adverse social climates, and system risks
- Offenders are “disgruntled”
- Separation of duties always
- Terminate with extreme professionalism
- Monitor Remote Access
- Effective pre-job screening
- Security Awareness
- Consistent enforcement



- Insider threats are a complex risk
- Effective Governance of Insider Threats is important
- Technical Controls serve effective management
- Proper processes avert occurrence and limit damage

